Amendments to the Claims

This listing of the claims replaces all prior versions and listing of the claims in the present application.

Listing of Claims

1. (currently amended) A security system for repelling malicious softwares in computers and computer networks and that is ~~adapted~~ configured to forward messages, the security system comprising a first sub-system to detect unknown malicious softwares having one or more characteristics unknown to said first sub-system, said first sub-system being configured, ~~adapted~~ in connection with the forwarding of messages or with other action or, in a timed manner, to perform at least a partial simulation ~~one or more predetermined actions~~ to activate unknown malicious softwares having one or more characteristics unknown to said first sub-system and to detect the activated unknown malicious softwares by detecting consequences of activation of the unknown malicious softwares.

2. (previously presented) The security system in accordance with Claim 1, that is adapted to forward an alarm caused by the detection of the malicious softwares to at least one system connected to the security system.

3. (previously presented) The security system in accordance with Claim 1, that is further adapted to break a

connection to at least one other system on the basis of an alarm caused by the detection of the malicious softwares.

4. (previously presented) The security system in accordance with Claim 1, further comprising a second sub-system for forwarding messages from the first sub-system to at least one system connected to the security system.

5. (previously presented) The security system in accordance with Claim 1, further comprising a third sub-system that is adapted to break a connection to at least one other sub-system upon receiving an alarm.

6. (previously presented) The security system in accordance with Claim 5, wherein the at least one other sub-system includes an identifier which corresponds to an identifier of the third sub-system.

7. (canceled)

8. (previously presented) The security system in accordance with Claim 2, wherein the alarm is a message or at least a part of a message that is forwarded to the recipient prior to other communications.

9. (previously presented) The security system in accordance with Claim 5, wherein the third sub-system includes at least one computer or one network element including a computer.

10. (previously presented) The security system in accordance with Claim 2, wherein the alarm is forwarded via a separate connection.

11. (canceled)

12. (previously presented) The security system in accordance with Claim 1, wherein the consequences of activation of the malicious softwares detected by the first sub-system include at least one of: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect the malicious softwares, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there.

13. (canceled)

14. (previously presented) The security system in accordance with Claim 1, wherein the first sub-system is adapted to choose one or more of the following logics when trying to activate the malicious softwares: one defined by the user, pre-programmed or at least partially random logic.

15. (previously presented) The security system in accordance with Claim 5, further comprising a parallel system that is adapted to save a message sent from the third sub-system, the parallel system being connected in parallel with the third sub-system.

16. (previously presented) The security system in accordance with Claim 15, wherein the first sub-system is adapted to compare in the parallel system a message sent from the third sub-system to the first sub-system and additionally saved in the parallel system in order to detect an anomaly caused by a malicious software.

17. (previously presented) The security system in accordance with Claim 15, wherein the parallel system is adapted to forward a message saved by it.

18. (previously presented) The security system in accordance with Claim 1, that is adapted to examine messages forwarded through the security system in order to detect known malicious softwares.

19. (previously presented) The security system in accordance with Claim 4, comprising first and second ones of the at least one system, wherein the security system is adapted to transfer data between the first and the second ones of the at least one system through the first and the second sub-systems, and wherein the security system is adapted to disrupt the connection between the first one of the at least one system and the first sub-system before a connection is established between the first and the second sub-systems and to disrupt the connection between the first and the second sub-systems before a connection is established between the second sub-system and the second one of the at least one system.

20. (previously presented) The security system in accordance with claim 1, wherein said first sub-system is adapted to compare messages with at least partially identical identifiers with each other in order to detect unknown malicious softwares.

21. (previously presented) The security system in accordance with Claim 20, wherein the first sub-system is adapted to request the sender of the messages with at least partially identical identifiers to re-send at least one of the messages and is further adapted to compare at least one re-sent message received with the original messages in order to detect messages containing malicious softwares.

22. (currently amended) A method for repelling malicious softwares in computers and data networks, the method being carried out in a security system including a first sub-system for forwarding messages and for detecting malicious softwares having one or more characteristics unknown to said first sub-system and that is isolatable from a remainder of the security system, the method includes the steps where:

- functions of the security system are monitored by the first sub-system in order to detect consequences of activation, in an at least partial simulation, of an unknown malicious software having one or more characteristics unknown to said first sub-system, when consequences of activation including at least one of the following: a change takes place in the first sub-system prior to actions causing changes carried out by the first

sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a malicious software, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there,

- a malicious ~~softwares~~ software is detected when one of the consequences is detected, and

- an alarm is given.

23. (currently amended) A method for repelling malicious softwares in computers and computer networks, the method comprising the steps of:

~~taking one or more predetermined actions~~ performing an at least partial simulation to activate unknown malicious softwares having one or more characteristics unknown to an entity performing the method in connection with the forwarding of messages or other action, or in a timed manner,

detecting the activated unknown malicious softwares by detecting consequences of activation of the malicious softwares caused by the at least partial simulation ~~one or more predetermined actions~~, and

giving an alarm when a malicious software is detected.

24-25. (canceled)

26. (previously presented) The method in accordance with Claim 23, wherein the method is run in a security system including a first sub-system and a second sub-system and wherein the consequences of activation of the malicious software include at least one of: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a malicious software, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there.

27-28. (canceled)

29. (previously presented) The method in accordance with Claim 23, further comprising the step where known malicious softwares are searched for on the basis of their characteristics.

30. (previously presented) The method in accordance with Claim 26, wherein the security system is connected to a first system and a second system and wherein data are transferred between the first system and the second system through the first sub-system and the second sub-system phase by phase in order, in which phases:

- the connection for data transfer is disrupted between the first system and the first sub-system,

- a connection for data transfer is established between the first sub-system and the second sub-system,

- the connection for data transfer is disrupted between the first sub-system and the second sub-system,

- a connection for data transfer is established between the second sub-system and the second system.

31. (currently amended) An apparatus for repelling malicious softwares in computers and computer networks, comprising equipment for saving data and for handling data and equipment for transferring data with another apparatus, wherein the apparatus is ~~adapted~~ configured to receive a message and to perform an at least partial simulation ~~one or more predetermined actions~~ to activate unknown malicious softwares having one more characteristics unknown to the apparatus and contained in the message and to detect the activated unknown malicious softwares by detecting consequences of activation of the malicious softwares.

32. (canceled)

33. (previously presented) The apparatus in accordance with Claim 31, wherein the consequences of activation of the malicious software include at least one of: a change takes place prior to actions caused by changes made by the apparatus, a change takes place that is not an action taken by the apparatus to detect a malicious software.

34. (previously presented) The apparatus in accordance with Claim 31, wherein the apparatus is adapted to send a message to either a sub-assembly of the apparatus or to said another apparatus, and wherein the consequences of activation of the malicious software include at least one of: a message leaves without authorization from the anti-malicious software of the apparatus, a message leaves for an address it has not originally been directed to, a message does not leave although it has been given a command to be sent.

35-36. (canceled)

37. (previously presented) The apparatus in accordance with Claim 31, wherein the apparatus examines the message in order to detect known malicious softwares.

38. (canceled)

39. (previously presented) A security system for repelling malicious software in a computer and that is adapted to forward messages, the security system comprising:

a first sub-system that detects unknown malicious software having one or more characteristics unknown to said first sub-system, said first sub-system being configured ~~adapted~~, in connection with forwarding of messages or with another action in a timed manner, to activate in an at least partial simulation an unknown malicious software having one or more characteristics unknown to said first sub-system and to detect the activated

unknown malicious software by detecting a consequence of the activation of the malicious software; and

an analyzing sub-system that receives files contaminated with an unknown malicious software from said first sub-system and that analyzes the unknown malicious software to provide fingerprints of the unknown malicious software and that forwards the fingerprints.

40. (previously presented) The security system in accordance with Claim 1, wherein the security system communicates with the computer network being protected by the security system, but is separate from the computer network.

41. (previously presented) The security system in accordance with Claim 40, wherein the security system is in a gateway for the computer network.